WHAT IS CLAIMED IS:

1. A method for a client device to regulate access to different networks, the method comprising:

obtaining information to identify adapters connected to a particular client device and networks to which said adapters are connected;

generating a profile for each network, including a current network to which said particular client device is connected;

comparing said profile of said current network to previously generated profiles to determine if said particular client device has previously connected to said current network; and

if said particular client device has previously connected to said current network, applying security settings previously utilized for said current network for regulating access to said current network.

2. The method of claim 1, further comprising:

determining the security settings to be applied for said current network if said particular client device has not previously connected to said current network; and

applying said security settings for regulating access to said current network.

3. The method of claim 2, further comprising:

storing said security settings for said current network; and

automatically applying said security settings when said particular client device subsequently connects to said current network.

4. The method of claim 2, wherein said step of determining the security settings to be applied for said current network includes applying an established policy.

5. The method of claim 4, wherein said established policy includes treating a current network to which said device has not previously connected as untrusted.

6. The method of claim 4, wherein said established policy includes treating a current network to which said device has not previously connected as trusted.

7. The method of claim 4, wherein said established policy includes obtaining user input regarding said security settings.

8. The method of claim 7, wherein said established policy includes security settings to be applied in the event that said user input is not obtained.

9. The method of claim 1, wherein said security settings are applied to a firewall module for regulating access to said current network.

10. The method of claim 1, wherein said step of obtaining information to identify adapters and networks is initiated each time said particular client device is connected to a network.

11. The method of claim 1, wherein information to identify adapters and networks is obtained from an operating system kernel facility.

12. The method of claim 11, wherein changes to network information in said operating kernel facility are examined to determine if the configuration of an adapter has changed.

13. The method of claim 11, wherein changes to network information in said operating kernel facility are examined to determine if said current network has changed.

14. The method of claim 1, wherein a list of all adapters is constructed upon connection of said particular client device to a network.

15. The method of claim 14, wherein each said adapter's network configuration is constructed upon connection of said particular client device to a network.

16. The method of claim 14, wherein a profile of all adapters and said adapters' network configuration is constructed each time said particular client device is connected to a network.

17. The method of claim 16, wherein said profile of an adapter includes a selected one or more of: connection method, physical address, IP address, subnet mask, and gateway IP address.

18. The method of claim 16, wherein said profile of an adapter's network configuration includes a selected one or more of: network IP address, network mask, gateway MAC address, and connection name.

19. The method of claim 1, wherein a profile of said adapters and networks connected to said adapters is constructed each time a change in said adapters' network configuration is detected.

20. The method of claim 1, wherein a network is identified by connection name if said network is a dialup connection with a resolvable connection name.

21. The method of claim 1, wherein a network is identified by connection name if said network is a PPP over Ethernet (PPPoE) connection with a resolvable connection name.

22. The method of claim 1, wherein a network is identified by gateway IP address and subnet mask if said network is an Ethernet network with a public IP address.

23. The method of claim 1, wherein a network is identified by gateway IP address, subnet mask and physical address if said network is an Ethernet network with a private IP address.

24. The method of claim 23, wherein said physical address is a MAC address.

25. The method of claim 1, wherein a network is identified by gateway IP address and subnet mask if said network is a token ring network.

26. The method of claim 1, wherein a network is identified by gateway IP address and subnet mask if said network is an infrared network.

27. The method of claim 1, wherein a unique identifier is assigned to each network that is profiled.

28. The method of claim 27, wherein said unique identifier is based upon a selected one or more of connection name, gateway IP address, subnet mask and physical address.

29. The method of claim 27, wherein each said unique identifier is stored.

30. The method of claim 27, wherein said unique identifier for a current network that is identified is compared to prior identifiers to determine if said particular client device has previously connected to said current network.

31. A method for a device to identify different networks to which said device is connected, the method comprising:

obtaining information to identify adapters connected to said device and current networks to which said adapters are connected;

generating a profile for said current networks, including a current network to which said device is connected;

comparing said profile of said current network to which said device is connected to prior profiles to determine if said device has previously connected to said current network; and

if said device has not previously connected to said current network, automatically notifying the user of said device of said connection to said current network.

32. The method of claim 31, further comprising:

if said device has not previously connected to said current network, obtaining user input on the security settings to be applied for said current network.

33. The method of claim 32, further comprising:

applying said security settings to regulate access to said device.

34. The method of claim 33, wherein said security settings are applied to a firewall module for regulating access to said device.

35. The method of claim 32, further comprising:

storing said security settings; and

applying said security settings in the event said device subsequently connects to said current network.

36. The method of claim 31, further comprising:

if said device has previously connected to said current network, applying the security settings previously utilized for said current network for regulating access to said device.

37. The method of claim 31, wherein said profiles of said current networks are used by a policy management application.

38. The method of claim 31, wherein said profiles of said current networks are used by a security management application.

39. The method of claim 31, wherein said profiles of said current networks are used by an end point security product to regulate access to said device.

40. A method for a device to identify different networks to which said device is connected, the method comprising:

obtaining information to identify a current network to which said device is connected;

generating a profile for said current network;

comparing said profile of said current network to previously generated profiles to determine if said device has previously connected to said current network; and

if said device has not previously connected to said current network, automatically treating said current network as untrusted for purposes of regulating access to said device.

41. The method of claim 40, wherein a firewall module regulates access to said device.

42. The method of claim 40, further comprising:

notifying the user of said device if said device has not previously connected to said current network.

43. The method of claim 42, further comprising:

obtaining user input on the security settings to be applied to regulate access to said device.

44. The method of claim 43, further comprising:

automatically applying said security settings to a firewall module to regulate access to said device.

45. A method for a device to identify different networks to which said device is connected, the method comprising:

obtaining information to identify a current network to which said device is connected;

generating a profile for said current network;

comparing said profile of said current network to previously stored profiles to determine if said device has previously connected to said current network; and

if said device has not previously connected to said current network, automatically treating said current network as trusted for purposes of regulating access to said device.

46. The method of claim 45, wherein a firewall module regulates access to said device.

47. The method of claim 45, further comprising:

notifying the user of said device if said device has not previously connected to said current network.

48. The method of claim 47, further comprising:

obtaining user input on the security settings to be applied to regulate access to said device.

49. The method of claim 48, further comprising:

automatically applying said security settings to a firewall module to regulate access to said device.

50. A system for a device to identify different networks to which said device is connected and regulate access to said device, the system comprising:

a network information engine for obtaining and processing information on networks to which said device is connected;

a network information data structure for storing said information on said networks; and

a zone configuration module for establishing security settings to regulate access to said device.

51. The system of claim 50, wherein said network information engine constructs a list of all connected adapters upon connection of said client device to a network.

52. The system of claim 51, wherein said network information engine constructs a list of all networks connected to said adapters upon connection of said device to a network.

53. The system of claim 51, wherein said network information engine constructs a list of all adapters and networks to which said adapters are connected each time a change in said current network is detected.

54. The system of claim 50, wherein said network information engine obtains information to identify adapters connected to said device from an operating system kernel facility.

55. The system of claim 54, wherein said network information engine obtains information to identify networks connected to said adapters from said operating system kernel facility.

56. The system of claim 54, wherein changes to network information in said operating kernel facility are examined to determine if a current network to which said device is connected has changed.

57. The system of claim 50, wherein said network information engine identifies a network by connection name if said network is a dialup connection with a resolvable connection name.

58. The system of claim 50, wherein said network information engine identifies a network by connection name if said network is a PPPoE connection with a resolvable connection name.

59. The system of claim 50, wherein said network information engine identifies a network by gateway IP address and subnet mask if said network is an Ethernet network with a public IP address.

60. The system of claim 50, wherein said network information engine identifies a network by gateway IP address, subnet mask and physical address if said network is an Ethernet network with a private IP address.

61. The system of claim 60, wherein said physical address is a MAC address.

62. The system of claim 50, wherein said network information engine identifies a network by gateway IP address and subnet mask if said network is a token ring network.

63. The system of claim 50, wherein said network information engine identifies a network by gateway IP address and subnet mask if said network is an infrared network.

64. The system of claim 50, wherein said network information engine assigns a unique identifier to each network.

65. The system of claim 64, wherein said network information engine constructs said unique identifier based upon a selected one or more of connection name, gateway IP address, subnet mask and physical address.

66. The system of claim 64, wherein each said unique identifier is stored in said network information data structure.

67. The system of claim 64, wherein each said unique identifier is stored in a database.

68. The system of claim 64, wherein said network information engine compares said unique identifier for a current network to previously stored identifiers to determine if said device has previously connected to said current network.

69. The system of claim 50, wherein said zone configuration module stores security settings for regulating access to said device.

70. The system of claim 69, wherein said security settings include whether to treat a network as trusted.

71. The system of claim 69, wherein said security settings include whether to treat a network as untrusted.

72. The system of claim 69, wherein said security settings include treating a current network to which said device has not previously connected as untrusted.

73. The system of claim 69, wherein said security settings include obtaining user input regarding the security settings to be applied for a network.

74. The system of claim 73, wherein said security settings include rules to be applied in the event that user input is not obtained.

75. The system of claim 50, wherein said zone configuration module stores security settings for regulating access from said device to different networks.

76. The system of claim 50, wherein said zone configuration module automatically applies said security settings to a firewall module for purposes of regulating access to said device.

77. The system of claim 50, further comprising:

a firewall module for regulating access to and from said device.

78. The system of claim 77, wherein said zone configuration module automatically applies said security settings to said firewall module for purposes of regulating access to said device.